53.

Cohomologie galoisienne des groupes algébriques linéaires

Colloque sur la théorie des groupes algébriques, Bruxelles (1962), 53–68

A tout groupe algébrique G sur un corps k, on peut associer l'ensemble $H^1(k, G)$ des classes d'espaces principaux homogènes sur G qui sont définis sur k (cf. Weil [23] ainsi que Lang-Tate [17]). Lorsque G est un groupe «classique», $H^1(k, G)$ a une interprétation non moins classique; ainsi, si G est le groupe projectif $\boldsymbol{PGL_n}$, $H^1(k, G)$ s'identifie à la partie du groupe de Brauer de k formée des éléments décomposés par une extension de k dont le degré divise n (cf. [20], Chap. X); si G est le groupe orthogonal d'une forme quadratique non dégénérée Q, les éléments de $H^1(k, G)$ correspondent bijectivement aux classes de formes quadratiques non dégénérées sur k qui ont même rang que Q; etc. Jusqu'à présent, ces cas particuliers ont été étudiés séparément. Lorsqu'on essaie d'unifier les résultats obtenus, pour avoir des énoncés valables pour tout groupe linéaire, ou tout groupe semi-simple, on est amené à formuler un certain nombre de *conjectures*; ce sont ces conjectures que je me propose de discuter.

Je me bornerai au cas des groupes *linéaires*; les variétés abéliennes posent des problèmes tout aussi intéressants, mais d'un genre différent.

§ 1. Rappels

1.1. *Cohomologie galoisienne*

Soit k un corps, et soit G un groupe algébrique sur k, autrement dit un groupe dans la catégorie des schémas algébriques sur k (cf. Grothendieck [12], Chap. I, § 6.4). On supposera dans tout ce qui suit que le schéma de G est *simple sur* k ([11], § II); comme G est un groupe, cela revient à dire que, pour toute extension k' de k, le faisceau d'anneaux de $G \otimes_k k'$ n'a pas d'éléments nilpotents. La composante connexe de l'élément neutre de G est alors un «groupe algébrique défini sur k», au sens de Weil.

Si K est une extension de k, nous noterons G_K le groupe des points de G à valeurs dans K (ou, comme on dit, des points de G «rationnels sur K»). Si K/k est galoisienne, de groupe de Galois $\mathfrak{g}$, le groupe $\mathfrak{g}$ opère sur G_K; il opère même continûment, si l'on munit G_K de la topologie discrète, et $\mathfrak{g}$ de sa topologie naturelle de groupe de Galois; si $s \in \mathfrak{g}$ et $x \in G_K$, nous noterons $s(x)$, ou ${}^s x$ le transformé de x par s. L'ensemble $H_0(\mathfrak{g}, G_K)$ des éléments de G_K invariants par $\mathfrak{g}$ s'identifie à G_k. On définit $H^1(\mathfrak{g}, G_K)$ de la manière suivante (cf. Lang-Tate [17], ou [20], p. 131) : un *cocycle* est une application continue $s \to x_s$ de $\mathfrak{g}$ dans G_K telle que $x_{st} = x_s {}^s x_t$; deux cocycles x_s et x'_s sont dits *cohomologues* s'il existe $a \in G_K$ tel que $x'_s = a^{-1} x_s {}^s a$; c'est là une relation d'équivalence entre cocycles, et les classes de cette relation d'équivalence sont par définition les éléments de $H^1(\mathfrak{g}, G_K)$; l'ensemble $H^1(\mathfrak{g}, G_K)$ contient un élément canonique, noté indifféremment 0 ou 1 (il correspond au cocycle x_s égal à 1 pour tout $s \in \mathfrak{g}$). Lorsque G est commutatif, $H^1(\mathfrak{g}, G_K)$ a une structure naturelle de groupe abélien; de plus, on définit par le procédé habituel les groupes de cohomologie supérieurs $H^i(\mathfrak{g}, G_K)$. On écrit souvent $H^i(K/k, G)$ au lieu de $H^i(\mathfrak{g}, G_K)$; on a $H^i(K/k, G) = \varinjlim \cdot H^i(K_\alpha/k, G)$, lorsque K_α parcourt l'ensemble des sous-extensions galoisiennes *finies* de K.

Le cas le plus intéressant est celui où l'on prend pour K la *clôture séparable* k_s de k; les $H^i(k_s/k, G)$ sont alors notés $H^i(k, G)$.

Remarque. Lorsque le groupe G n'est pas simple sur K, $H^1(k_s/k, G)$ ne coïncide pas nécessairement avec la «vraie» cohomologie de G, définie par Cartier et Grothendieck (voir [10]); de tels groupes s'introduisent nécessairement, par exemple lorsque l'on veut étudier des isogénies inséparables sur un corps imparfait.

1.2. *Formes*

Soit V un schéma algébrique sur k, et supposons que G soit le groupe des automorphismes de V (en ce sens que, pour toute extension K/k, G_K est le groupe d'automorphismes de $V \otimes_k K$).

Soit K/k une extension, et soit V' un schéma algébrique sur k; on dit que V' est une *K/k-forme* de V si $V \otimes_k K$ et $V' \otimes_k K$ sont K-isomorphes (i.e. si V et V' «deviennent isomorphes sur K»). Supposons que K/k soit galoisienne, de groupe de Galois $\mathfrak{g}$, et que V soit quasi-projective; alors *les classes de K/k-formes de V* (pour la relation d'équivalence définie par l'isomorphisme) *correspondent bijectivement aux éléments de* $H^1(K/k, G)$. La correspondance se définit de la manière suivante : si V' est une K/k-forme de V, on choisit un isomorphisme $f : V \otimes_k K \to V' \otimes_k K$, et à tout $s \in \mathfrak{g}$ on fait correspondre $x_s = f^{-1} \circ {}^s f$, qui est un élément de G_K; on obtient ainsi un cocycle x_s dont la classe ne dépend pas du choix de f; deux K/k-formes définissent des cocycles cohomologues si et seulement si elles sont isomorphes. Réciproquement, tout cocycle x_s correspond à une K/k-forme V_x de V (on dit parfois que V_x se déduit de V en «tordant V au moyen de x»); cela se voit en utilisant les théorèmes de descente du corps de base de Weil (ce qui revient à faire opérer $\mathfrak{g}$ dans $V \otimes_k K$ et à passer au quotient); c'est là que l'hypothèse de quasi-projectivité intervient. Lorsque l'on prend $K = k_s$, on parle simplement d'une *k-forme* de V; les classes de k-formes correspondent donc aux éléments de $H^1(k, G)$, du moins si V est quasi-projective.

La correspondance entre formes et classes de cohomologie s'applique aussi lorsque les variétés considérées sont munies de *structures* de groupes (ou d'espaces homogènes, ou d'algèbres, etc.), G_K étant alors le groupe des automorphismes de $V \otimes_k K$ muni de la structure en question; la démonstration est la même (bien entendu, il faut vérifier dans chaque cas que l'espèce de structure considérée est compatible avec la descente du corps de base dans une extension galoisienne).

Exemple : prenons pour V le groupe G, et munissons-le de sa structure naturelle d'*espace principal homogène* sur G; le groupe d'automorphismes est G lui-même. Comme G est quasi-projectif, on retrouve le résultat connu (cf. Lang-Tate [17]) selon lequel les éléments de $H^1(K/k, G)$ correspondent bijectivement aux classes d'espaces principaux homogènes sur G qui ont un point rationnel dans K.

On trouvera d'autres exemples dans [20], Chap. X, et dans Hertzig [13].

1.3. *Propriétés formelles des H^i*

On va se borner à en citer quelques-unes :

1.3.1. Soit K/k une extension finie séparable, soit G un groupe algébrique sur K, et soit $H = R_{K,k}(G)$ le groupe algébrique sur k obtenu à partir de G par restriction du corps de base au sens de Weil ([24], p. 4).

On a alors des bijections canoniques :

$$H^i(k, H) \to H^i(K, G)$$

pour $i = 0, 1$ (et même pour tout i si G est commutatif).

1.3.2. Soit H un sous-groupe de G, et soit $x = (x_s)$ un cocycle dans G. Pour que x soit cohomologue à un cocycle de H, il faut et il suffit que le schéma $V = (G/H)_x$, obtenu en tordant G/H au moyen de x, ait un point à valeurs dans k.

1.3.3. Si H est un sous-groupe invariant de G, on a un analogue non commutatif de la suite exacte de cohomologie; cf. [20] p. 131-134, qui est d'ailleurs très incomplet; il n'y a heureusement aucune difficulté à le compléter, en se guidant sur le cas topologique pour lequel on dispose des exposés de Dedecker [6], Frenkel [8] et Grothendieck [9].

§ 2. Corps de dimension $\leqslant 1$

2.1. *Définition*

Soit k un corps. Nous dirons que k est *de dimension* $\leqslant 1$ (ce que nous écrirons $d(k) \leqslant 1$) si, pour toute extension algébrique K de k, le *groupe de Brauer B_K de K est nul*; il suffit d'ailleurs que $B_K = 0$ pour toute extension *finie* K de k (1).

Cette condition équivaut à la suivante (cf. [20], p. 169, prop. 11) :

(*) *Si $L \supset K$ sont deux extensions finies de k, avec L séparable sur K, on a $N_{L/K}(L^*) = K^*$.*

(1) Il suffit même que B_K soit nul pour toute extension finie et *séparable* K de k. En effet, toute extension finie L de k est radicielle sur une telle extension K, et, d'après un théorème de Hochschild, l'homomorphisme $B_K \to B_L$ est surjectif; d'où $B_L = 0$.

Le terme de «dimension» est justifié (au moins pour un corps parfait) par le résultat suivant :

PROPOSITION 2.1. *Soit k_s la clôture séparable de k, soit $\mathfrak{g}$ le groupe de Galois de k_s/k, et soit $cd(\mathfrak{g})$ la dimension cohomologique de* $\mathfrak{g}$ (au sens de Tate, cf. [7]). *Si k est de dimension $\leqslant 1$, on a $cd(\mathfrak{g}) \leqslant 1$ et la réciproque est vraie si k est parfait.*

[On rappelle que $cd(\mathfrak{g})$ est le plus petit entier n tel que $H^{n+1}(\mathfrak{g}, A) = 0$ pour tout $\mathfrak{g}$-module fini A (commutatif, bien entendu).]

Si $d(k) \leqslant 1$, on a $cd(\mathfrak{g}) \leqslant 1$ d'après le théorème 4.2 de [7]. Si k est parfait, k_s^* est un groupe *divisible*; si $cd(\mathfrak{g}) \leqslant 1$, on voit tout de suite que cela entraîne $H^2(\mathfrak{g}, k_s^*) = 0$, autrement dit $B_k = 0$. En appliquant le même argument à une extension finie de k, ce qui est licite vu la prop. 3.2 de [7], on voit bien que k est de dimension $\leqslant 1$.

2.2. *Exemples de corps de dimension $\leqslant 1$*

2.2.1. Un corps fini.

2.2.2. Une extension de degré de transcendance 1 d'un corps algébriquement clos.

2.2.3. Un corps local (i.e. complet pour une valuation discrète) à corps résiduel algébriquement clos; plus généralement, l'extension maximale non ramifiée d'un corps local à corps résiduel parfait.

2.2.4. Une extension algébrique de $\boldsymbol{Q}$ contenant toutes les racines de l'unité.

Pour les démonstrations (ou les références à la bibliographie), voir [20], p. 170.

2.3. *Corps* (C_1)

Ce sont ceux qui vérifient la propriété suivante (cf. Lang [14]) :

(C_1) — *Toute équation homogène $f(x_1, \ldots, x_n) = 0$, de degré $d < n$, a une solution non triviale dans k.*

On sait que $(C_1) \Rightarrow d(k) \leqslant 1$ (cf. [20], p. 169, prop. 10). La réciproque est inexacte; en effet, si k est de caractéristique $p \neq 0$, la condition (C_1) entraîne que $[k : k^p] \leqslant p$ (considérer une p-base de k), et il est facile de construire des corps de dimension $\leqslant 1$ mettant en défaut cette condition (clôture séparable d'un corps de fonctions à deux variables). Il n'est pas exclu que, pour les corps k

tels que $[k : k^p] \leqslant p$, la condition (C_1) soit équivalente à la con-
1 dition $d(k) \leqslant 1$, mais c'est peu probable.

Les exemples 2.2.1, 2.2.2 et 2.2.3 du nº précédent vérifient (C_1), cf. Lang [14]; on ignore s'il en est de même de l'exemple 2.2.4.

2.4. *Première conjecture*

Conjecture I. *Si k est un corps parfait de dimension $\leqslant 1$,*
2 *et si G est un groupe linéaire connexe défini sur k, on a $H^1(k, G) = 0$* (2).

Cette conjecture est démontrée dans les cas suivants :

a) *Si k est un corps fini* (Lang [15]); dans ce cas, l'hypothèse que G est un groupe linéaire est inutile.

b) *Si k est de caractéristique zéro et vérifie* (C_1) (cf. l'exposé de Springer à ce colloque).

c) *Si G est résoluble, ou si c'est un groupe semi-simple «classique»* (cf. § 3).

On peut raisonnablement espérer que la démonstration de Springer peut être transposée en caractéristique $p \neq 0$; le fait qu'il doive remplacer l'hypothèse $d(k) \leqslant 1$ par (C_1) n'est pas gênant pour les applications : les corps de dimension $\leqslant 1$ les plus importants vérifient bien (C_1), cf. nº 2.2.

Remarques

1) Inversement, si $H^1(k, G) = 0$ pour tout groupe semi-simple G, on a $d(k) \leqslant 1$. En effet, soit K une extension séparable finie de k, soit n un entier, et soit G le groupe $R_{K/k}(\boldsymbol{PGL}_n)$, obtenu à partir du groupe projectif $\boldsymbol{PGL}_n$ par restriction du corps de base de K à k (cf. nº 1.3.1); comme $H^1(k, G) = 0$, on voit que $H^1(K, \boldsymbol{PGL}_n) = 0$, et, puisque ceci est vrai pour tout n, on en déduit $B_K = 0$ (cf. [20], Chap. X), d'où $d(k) \leqslant 1$.

2) Si l'on abandonne l'hypothèse que k est parfait, on peut seulement conjecturer que $H^1(k, G) = 0$ lorsque G est *réductif*
3 connexe. On peut en effet construire des groupes unipotents dont la cohomologie est non nulle; par exemple, si $k = k_0((t))$, k_0 étant un corps de caractéristique p non nulle, le sous-groupe G de $\boldsymbol{G}_a \times \boldsymbol{G}_a$ défini par l'équation $y^p - y = tz^p$ est tel que

(2) Lang m'a signalé que cette conjecture lui avait été communiquée par Adelberg il y a plusieurs années.

$H^1(k, G) \neq 0$ (si $p \neq 2$ — on peut construire des exemples analogues pour $p = 2$).

2.5. *Conjectures supplémentaires*

La conjecture I ci-dessus me paraît extrêmement probable. Les deux suivantes sont plus hasardeuses :

4 CONJECTURE I′. *Soit k un corps parfait de dimension $\leqslant 1$, et soit G un groupe linéaire connexe défini sur k. Tout espace homogène sur G qui est défini sur k possède un point rationnel sur k.*

(Bien entendu, si X est l'espace homogène en question, on suppose que l'application de $G \times X$ dans X est définie sur k.)

Cette conjecture est plus forte que la conjecture I, comme on le voit en l'appliquant au cas d'un espace homogène *principal*.

CONJECTURE I″. *Soit k un corps parfait de dimension $\leqslant 1$, et soit $f : G \rightarrow G'$ un homomorphisme de groupes algébriques (définis sur k, ainsi que f). Si f est surjectif, l'application $H^1(k, G) \rightarrow H^1(k, G')$ induite par f est surjective.*

Ces deux conjectures sont vraies lorsque k est un *corps fini* : la première a été démontrée par Lang [15], et la seconde est immédiate. Dans le cas général, elles paraissent nettement plus difficiles que la conjecture I; la conjecture I″, appliquée au cas où G et G' sont finis, entraîne que le groupe de Galois de k_s/k possède une *propriété de relèvement* très stricte, qui l'apparente à un groupe libre.

§ 3. DÉMONSTRATION DE LA CONJECTURE I POUR DIVERS GROUPES

3.1. *Réduction au cas semi-simple*

PROPOSITION 3.1.1. *Si k est parfait, et si G est unipotent connexe, on a $H^1(k, G) = 0$.*

Comme k est parfait, G admet une suite de composition dont les quotients successifs sont isomorphes au groupe additif G_a (cf. Rosenlicht [19], cor. 2 à la prop. 5); comme l'on sait que $H^1(k, G_a) = 0$ (cf. [20], p. 158), on en déduit bien que $H^1(k, G) = 0$.

PROPOSITION 3.1.2. *Si k est de dimension $\leqslant 1$, et si G est un tore, on a $H^1(k, G) = 0$.*

On sait (cf. Ono [18], prop. 1.2.1) qu'il existe une extension galoisienne finie K/k telle que G soit K-isomorphe à un produit de groupes multiplicatifs $\boldsymbol{G}_m$. Si L/k est une extension galoisienne de k contenant K, de groupe de Galois $\mathfrak{g}$, le groupe $\mathfrak{g}$ opère sur le groupe X des *caractères* de G, et aussi sur le groupe $Y = \mathrm{Hom}\,(X, \boldsymbol{Z})$; le groupe G_L s'identifie de façon naturelle au produit tensoriel $L^* \otimes Y$. Comme $d(k) \leqslant 1$, L^* est un $\mathfrak{g}$-module cohomologiquement trivial (cf. [20], p. 169, prop. 11), et d'après le théorème de Nakayama, il en est de même de $L^* \otimes Y$ (*loc. cit.*, p. 170). On a donc $H^1(L/k, G) = 0$, et en passant à la limite sur L on voit bien que $H^1(k, G) = 0$.

PROPOSITION 3.1.3. *Si k est parfait de dimension $\leqslant 1$, et si G est un groupe linéaire connexe résoluble défini sur k, on a $H^1(k, G) = 0$.*

Cela résulte des propositions précédentes, en remarquant qu'un tel groupe est extension d'un tore par un groupe unipotent connexe.

COROLLAIRE. *Pour démontrer la conjecture* I, *on peut se borner au cas des groupes semi-simples.*

Cela résulte de la proposition précédente et du fait que tout groupe linéaire connexe est extension d'un groupe semi-simple par un groupe résoluble connexe.

PROPOSITION 3.1.4. *Soit $f : G \to G'$ une isogénie de groupes linéaires connexes définis sur k. Si k est parfait de dimension $\leqslant 1$, l'application de $H^1(k, G)$ dans $H^1(k, G')$ définie par f est bijective.*

(Bien entendu, on suppose que f est définie sur k.)

Soit N le noyau de f; c'est un sous-groupe fini du centre de G; si k_s désigne la clôture algébrique de k, le groupe G'_{k_s} s'identifie au quotient G_{k_s}/N. Comme $d(k) \leqslant 1$, on a $H^2(k, N) = 0$, et la suite exacte de cohomologie (cf. [20], p. 133, prop. 2) montre que $H^1(k, G) \to H^1(k, G')$ est surjectif. Reste à voir que cette application est injective. Soient x et y deux éléments de $H^1(k, G)$ ayant même image dans $H^1(k, G')$; quitte à «tordre» G et G' au moyen d'un cocycle représentant x, on peut supposer que $x = 0$. D'après [20], *loc. cit.*, l'élément y provient d'un élément $z \in H^1(k, N)$, et l'on est ramené à démontrer que l'image de $H^1(k, N)$ dans $H^1(k, G)$ est nulle. Or, d'après Rosenlicht ([19], p. 45), il existe un sous-groupe de Cartan C de G rationnel sur k; ce sous-groupe contient N, et l'application $H^1(k, N) \to H^1(k, G)$ se factorise à travers $H^1(k, C)$. Mais C est nilpotent, donc *a fortiori* résoluble, et connexe; d'après la proposition 3.1.3, on a

$H^1(k, C) = 0$, et il s'ensuit bien que l'image de $H^1(k, N)$ dans $H^1(k, G)$ est nulle.

COROLLAIRE. *Pour démontrer la conjecture* I, *on peut se borner au cas des groupes semi-simples simplement connexes* (*ou adjoints. au choix*).

C'est évident.

3.2. *Nullité de la cohomologie pour les extensions quadratiques*

Démontrons d'abord un résultat général :

PROPOSITION 3.2.1. *Soit k un corps parfait infini, soit G un groupe linéaire connexe défini sur k, et soit K/k une extension galoisienne finie, de groupe de Galois $\mathfrak{g}$. Toute classe de cohomologie $\gamma \in H^1(K/k, G)$ peut être représentée par un cocycle c_s ($s \in \mathfrak{g}$, $c_s \in G_K$) tel que, pour tout $s \neq 1$, c_s soit un élément régulier de G_K (au sens de Chevalley,* [4], p. 7-03).

Soit x_s un cocycle représentant γ; nous devons montrer qu'il existe $a \in G_K$ tel que $c_s = a^{-1}\, x_s\, {}^s a$ soit régulier pour tout $s \neq 1$ dans $\mathfrak{g}$. Soit $H = R_{K/k}(G)$ le groupe obtenu à partir de G par restriction des scalaires de K à k (cf. nº 1.3.1) et soit p l'homomorphisme canonique de H dans G; on sait que p est défini sur K, et que la collection $\varphi = ({}^s p)$ de ses conjugués est un K-isomorphisme de H sur $G \times \ldots \times G$ (les facteurs de ce produit étant indexés par les éléments s de $\mathfrak{g}$). Soit U l'ensemble des éléments $b \in H$ tels que $p(b)^{\cdot -1} \cdot x_s {}^s p(b)$ soit régulier pour tout $s \neq 1$. En tenant compte de ce que φ est un isomorphisme, on voit que U est un ouvert non vide (pour la topologie de Zariski de H); d'après Rosenlicht ([19], p. 44), il s'ensuit que $H_k \cap U$ est non vide. Soit $b \in H_k \cap U$, et soit $a = p(b)$; on a $a \in G_K$, et ${}^s p(b) = {}^s a$; vu la définition de U, il s'ensuit bien que $a^{-1} x_s {}^s a$ est régulier pour tout $s \neq 1$.

PROPOSITION. 3.2.2. *Si K est une extension quadratique d'un corps parfait k de dimension $\leqslant 1$, et si G est un groupe linéaire connexe défini sur k, on a $H^1(K/k, G) = 0$.*

Notons $x \to \bar{x}$ l'automorphisme de G_K défini par l'automorphisme non trivial s de K/k. Un cocycle s'identifie à un élément $x \in G_K$ tel que $x \cdot \bar{x} = 1$. Vu la proposition précédente, on peut supposer que x est régulier (si k est fini, on sait de toutes façons que $H^1(K/k, G) = 0$). Soit C l'unique sous-groupe de Cartan de G qui contient x; il est défini sur K. Mais comme $\bar{x} = x^{-1}$, c'est aussi l'unique sous-groupe de Cartan contenant $\bar{x}$, ce qui montre qu'il est stable par s; il est donc en fait défini sur k. D'après la proposition 3.1.3, on a $H^1(k, C) = 0$ d'où *a fortiori* $H^1(K/k, C) = 0$; le cocycle x est cohomologue à zéro dans C, donc aussi dans G, cqfd.

Remarque. La proposition précédente s'étend au cas d'une extension galoisienne K/k dont le groupe de Galois est un 2-groupe; en effet, le corps K s'obtient par extensions quadratiques successives à partir de k, et l'on applique la proposition à chacune de ces extensions.

3.3. *Groupes classiques*

PROPOSITION 3.3.1. *Soit k un corps parfait de dimension $\leqslant 1$, et soit G un groupe semi-simple défini sur k, dont tous les facteurs simples* (sur la clôture algébrique de k) *sont de type $\boldsymbol{A}_n$, $\boldsymbol{B}_n$, $\boldsymbol{C}_n$ ou $\boldsymbol{D}_n$ (le type $\boldsymbol{D}_4$ étant exclu). Alors $H^1(k, G) = 0$.*

D'après la proposition 3.1.4, on peut supposer que G est un groupe *adjoint*; on peut aussi supposer qu'il est simple sur k, i.e. qu'il n'est pas décomposable en produit de façon non triviale sur le corps k. Cela n'implique pas nécessairement que G soit simple sur la clôture algébrique k_s de k; mais, si H désigne un facteur simple de G, et K/k le corps de rationalité de H, on voit tout de suite que G s'identifie à $R_{K/k}(H)$. Comme $H^1(k, G) = H^1(K, H)$, on est ramené à étudier le groupe H. En d'autres termes, on peut supposer que G est *simple* (sur k_s). Soit G_0 le groupe «de Tohoku», construit par Chevalley (cf. [3] ainsi que [5]), et de même type que G. Soit A le groupe d'automorphismes de G_0; comme G_0 est son propre groupe adjoint, on a une suite exacte

$$0 \to G_0 \to A \to E \to 0,$$

où E est un groupe fini (le groupe des automorphismes externes de G_0). On sait que E est cyclique d'ordre 1 ou 2 (grâce au fait que l'on a éliminé $\boldsymbol{D}_4$). Comme G est une k-forme de G_0, il est défini par un élément $g \in H^1(k, A)$, lequel a une image $e \in H(k, E)$; l'élément e peut être interprété comme un caractère d'ordre 1 ou 2 du groupe de Galois $\mathfrak{g}$ de k_s/k; il correspond à une extension K/k de degré 1 ou 2. Sur K, le groupe G est défini par un élément $g_K \in H^1(K, A)$ qui, cette fois, appartient à l'image de $H^1(K, G_0)$. Il en résulte en particulier que $H^1(K, G)$ est en correspondance bijective avec $H^1(K, G_0)$. Si l'on montre que $H^1(K, G_0)=0$, on en déduira que $H^1(K, G) = 0$, et comme on sait déjà que $H^1(K/k, G) = 0$ (cf. prop. 3.2.2), il en résultera bien que $H^1(k, G) = 0$.

Nous sommes donc ramené à montrer la nullité de $H^1(K, G_0)$ lorsque G_0 est un «groupe de Tohoku» de type $\boldsymbol{A}_n, \boldsymbol{B}_n, \boldsymbol{C}_n, \boldsymbol{D}_n$. De plus, la proposition 3.1.4 nous permet, si besoin est, de remplacer G_0 par un groupe isogène. Cela rend la vérification presque triviale : pour $\boldsymbol{A}_n$ (resp. $\boldsymbol{C}_n$), on remplace G_0 par $\boldsymbol{SL}_n$ (resp. par $\boldsymbol{Sp}_n$), et l'on sait que $H^1(K, \boldsymbol{SL}_n) = H^1(K, \boldsymbol{Sp}_n) = 0$ (cf. [20], Chap. X); pour $\boldsymbol{B}_n$ et $\boldsymbol{D}_n$, on remplace G_0 par le groupe spécial orthogonal correspondant $\boldsymbol{SO}(Q)$, et $H^1(K, \boldsymbol{SO}(Q))$ est l'ensemble des classes de formes quadratiques ayant même rang et même discriminant que Q (même invariant d'Arf si la caractéristique est 2 et si le rang est pair). Or, on sait que, pour tout couple de formes quadratiques Q, Q', non dégénérées et de même rang, il existe une extension L/K, composée d'extensions quadratiques, et telle que Q et Q' soient isomorphes sur L. Il s'ensuit que $H^1(K, \boldsymbol{SO}(Q))$ est réunion des $H^1(L/K, \boldsymbol{SO}(Q))$; comme ces derniers sont nuls (nº 3.2.2), on en déduit que $H^1(K, \boldsymbol{SO}(Q)) = 0$, ce qui achève la démonstration.

[La nullité de $H^1(K, \boldsymbol{SO}(Q))$ se déduit aussi sans difficultés des résultats de Witt [25] (en caractéristique $\neq 2$) et d'Arf [1] (en caractéristique 2).]

Remarques

1) Les types $\boldsymbol{G}_2$ et $\boldsymbol{F}_4$ doivent pouvoir se traiter par la même méthode, en utilisant l'interprétation de $\boldsymbol{G}_2$ (resp. $\boldsymbol{F}_4$) comme groupe d'automorphismes d'une algèbre d'octonions (resp. d'une algèbre de Jordan exceptionnelle).

2) Chevalley a démontré que le groupe d'automorphismes A introduit ci-dessus est produit *semi-direct* de G_0 par E : on peut réaliser E comme sous-groupe de A laissant stable un sous-groupe de Borel de G_0. Il en résulte que, *si $H^1(k, G) = 0$ pour toute forme G de G_0, l'application $H^1(k, A) \to H^1(k, E)$ est bijective*. La conjecture I entraîne donc que les formes de G_0, c'est-à-dire les groupes adjoints de même type que G_0, correspondent bijectivement aux éléments de $H^1(k,E)$, autrement dit aux homomorphismes du groupe de Galois de k_s/k dans E (à conjugaison près); lorsque k est fini, cela redonne un résultat de Hertzig [13]. Toujours en supposant

63

que k vérifie la conjecture I, le fait que E laisse stable un groupe de Borel de G_0 implique que *tout groupe semi-simple sur k possède un groupe de Borel défini sur k* (du point de vue Borel-Tits, il n'existe pas de groupe simple «anisotrope»); en fait, cette propriété est *équivalente* à la conjecture I (cf. l'exposé de Springer).

§ 4. Conjecture II

4.1. *Définitions*

Nous allons formuler diverses conditions, portant sur un corps k, et qui signifient plus ou moins que k «est de dimension $\leqslant 2$». La première est de nature cohomologique :

(H_2) — *Le groupe de Galois* $\mathfrak{g}$ *de* k_s/k *est de dimension cohomologique* $\leqslant 2$, *au sens de Tate* (cf. nº 2.1).

Voici des exemples de corps vérifiant (H_2) :

a) Un corps de nombres totalement imaginaire (Tate, non publié).

b) Une extension de degré de transcendance 1 d'un corps de dimension $\leqslant 1$; en particulier, un corps de fonctions à 2 variables sur un corps algébriquement clos, ou un corps de fonctions à 1 variable sur un corps fini.

c) Un corps local à corps résiduel parfait de dimension $\leqslant 1$; en particulier, un corps p-adique, ou un corps de séries formelles sur un corps fini.

La seconde condition est de nature diophantienne :

(C_2) — *Toute équation homogène* $f(x_1, \ldots, x_n) = 0$, *de degré d, telle que* $n > d^2$, *a une solution non triviale dans k.*

«Expérimentalement», ces deux conditions semblent très voisines : on ne connaît aucun exemple de corps parfait qui vérifie l'une et qui mette l'autre en défaut. Toutefois, on n'a démontré,
5 ni l'implication $(H_2) \Rightarrow (C_2)$ (du reste peu probable), ni l'implication $(C_2) \Rightarrow (H_2)$; la situation est franchement désagréable.

Enfin, voici la troisième condition :

(C_2') — *Toute extension finie K de k jouit des deux propriétés suivantes :*

(i) *Toute forme quadratique à 5 variables sur K représente zéro* (i.e. possède un vecteur isotrope non nul).

(ii) *Si D est un corps gauche fini sur K et de centre K, la norme réduite Nrd : $D^* \to K^*$ est surjective.*

Il est immédiat que $(C_2) \Rightarrow (C_2')$; l'avantage de (C_2') est qu'elle se vérifie beaucoup plus facilement. Par exemple, on sait que (C_2') est valable pour un corps de nombres totalement imaginaire, alors que la question analogue pour (C_2) paraît extrêmement difficile.

4.2. *Conjectures*

6 Conjecture II. *Si k est un corps parfait vérifiant (H_2), et si G est un groupe semi-simple simplement connexe défini sur k, on a* $H^1(k, G) = 0$ ([3]).

Vu l'incertitude où nous sommes sur «la bonne» définition d'un corps de dimension $\leqslant 2$, nous sommes forcés d'énoncer aussi :

Conjecture II bis (resp. II′ bis). *Même énoncé que la conjecture* II, *à cela près que la condition (H_2) est remplacée par la condition* (C_2) (resp. *par la condition* (C_2')).

Remarques

1) La conjecture II entraîne la conjecture I (appliquer le corollaire à la proposition 3.1.4).

2) Les conjectures II bis et II′ bis paraissent les plus accessibles à une vérification cas par cas; on en verra un exemple au n° suivant.

4.3. *Groupes semi-simples non simplement connexes*

Soit G un tel groupe, défini sur un corps parfait k, et soit $\bar{G}$ son revêtement simplement connexe. Soit A le noyau de $\bar{G} \to G$; la suite exacte de cohomologie (non abélienne) définit des applications cobords

$$\delta_0 : H^0(k, G) \to H^1(k, A) \quad \text{et} \quad \delta_1 : H^1(k, G) \to H^2(k, A).$$

Si la conjecture II s'applique au corps k et aux formes de $\bar{G}$, on voit que δ_1 est *injectif*, et δ_0 *surjectif*, ce qui fournit des renseignements sur $H^1(k, G)$.

([3]) Pour les corps p-adiques, cette conjecture m'a été communiquée par Martin Kneser, qui l'a vérifiée pour la plupart des groupes classiques.

Exemple : Prenons pour G un groupe spécial orthogonal (en caractéristique $\neq 2$); on a $\overline{G} = \boldsymbol{Spin}$, $A = \boldsymbol{Z}/2\boldsymbol{Z}$, $H^1(k, A) = k^*/k^{*2}$, tandis que $H^2(k, A)$ s'identifie au groupe des éléments α du groupe de Brauer de k tels que $2\alpha = 0$. L'homomorphisme δ_0 est la *norme spinorielle*; l'application δ_1 est en rapport étroit avec *l'invariant de Witt* des formes quadratiques (cf. Witt [25], ainsi que Springer [22]); il est facile de voir que δ_0 est surjective et δ_1 injective lorsque k vérifie (C_2'); on en conclut que la conjecture II'bis est valable pour un groupe ***Spin***.

§ 5. Compléments

5.1. *Corps p-adiques*

Si k est un corps p-adique et G un groupe linéaire défini sur k, on peut démontrer que $H^1(k, G)$ est *fini*; le même résultat vaut pour le corps $\boldsymbol{R}$ des nombres réels. Voir là-dessus un article en
7 collaboration avec A. Borel.

Il est probable que ce résultat de finitude reste valable sur un corps de séries formelles sur un corps fini, à condition de supposer en plus que G est *réductif*.

5.2. *Corps de nombres*

Soit k un corps de nombres (autrement dit une extension finie de $\boldsymbol{Q}$), soit I l'ensemble des topologies définies sur k par des valeurs absolues non triviales, et pour tout $i \in I$ soit k_i le complété de k; on sait que k_i est, soit un corps p-adique, soit $\boldsymbol{R}$, soit $\boldsymbol{C}$. Si G est un groupe algébrique défini sur k, notons G_i le groupe algébrique sur k_i défini par extension des scalaires à partir de G. Les injections $k \to k_i$ définissent une application

$$\omega : H^1(k, G) \to \prod_{i \in I} H^1(k_i, G_i).$$

Lorsque G est linéaire, cette application est *propre* : l'image réciproque d'un élément est finie (cf. Borel [2] pour le cas réductif). Pour certains groupes ω est même *injective* («principe de Hasse», cf. Lang [16]); les exemples les plus connus sont ceux des groupes projectifs et des groupes orthogonaux. Ce n'est malheureusement

pas là une propriété générale des groupes réductifs (ou même
8 semi-simples) comme on peut le voir sur des exemples.

Il reste toutefois la possibilité que les groupes *semi-simples simplement connexes* se comportent mieux. De façon précise, soit J le sous-ensemble de I formé des $i \in I$ tels que $k_i = \mathbf{R}$, et considérons l'application canonique

$$\pi : H^1(k, G) \to \prod_{i \in J} H^1(\mathbf{R}, G_i).$$

On peut conjecturer que π est *bijective* si G est semi-simple sim-
9 plement connexe. Noter que, si la conjecture de Kneser s'applique à G, on a $H^1(k_i, G_i) = 0$ pour $i \in I - J$, et π s'identifie à ω. Noter également que, si k est totalement imaginaire, J est vide, et l'on retombe sur un cas particulier de la conjecture II.

5.3. *Questions diverses*

(i) Comment se traduit en langage cohomologique le point de vue de Borel et Tits, ramenant la classification des groupes semi-simples à celle des groupes *anisotropes*?

(ii) Lorsque G est un groupe orthogonal, Springer [21] a démontré le résultat suivant : si K/k est une extension de degré impair, l'application canonique $H^1(k, G) \to H^1(K, G)$ est injective. Peut-on associer de même, à tout type de groupes semi-simples, un entier d tel que $H^1(k, G) \to H^1(K, G)$ soit injectif si le degré $[K : k]$ est premier à d?

BIBLIOGRAPHIE

[1] Arf, C., Untersuchungen über quadratische Formen in Körpern der Charakteristik 2 (*Journal de Crelle*, **183**, 1941, p. 148-167).

[2] Borel, A., Some properties of adele groups attached to algebraic groups (*Bull. Amer. Math. Soc.*, **67**, 1961, p. 583-585).

[3] Chevalley, C., Sur certains groupes simples (*Tohoku Math. Journal*, **7**, 1955, p. 14-66).

[4] Chevalley, C., Classification des groupes de Lie algébriques, séminaire ENS, 1956-58.

[5] Chevalley, C., Certains schémas de groupes semi-simples, séminaire Bourbaki, **13**, 1960-61, exposé 219.

[6] Dedecker, P., La structure algébrique de l'ensemble des classes d'espaces fibrés (*Bull. Acad. Roy. Belg.*, **42**, 1956, p. 270-290).

[7] Douady, A., Cohomologie des groupes compacts totalement discontinus, séminaire Bourbaki, **12**, 1959-60, exposé 189.

[8] Frenkel, J., Cohomologie non abélienne et espaces fibrés (*Bull. Soc. math. France*, **85**, 1957, p. 135-220).

[9] Grothendieck, A., A general theory of fibre spaces with structure sheaf (Univ. Kansas, Report n° 4, 1955).

[10] Grothendieck, A., Technique de descente et théorèmes d'existence en géométrie algébrique. I. Généralités. Descente par morphismes fidèlement plats, séminaire Bourbaki, **12**, 1959-60, exposé 190.

[11] Grothendieck, A., Séminaire de géométrie algébrique, IHES, 1960-61.

[12] Grothendieck, A., Eléments de géométrie algébrique (en collaboration avec J. Dieudonné), *Publ. Math. IHES*, 1960-61-62-...

[13] Hertzig, D., Forms of algebraic groups (*Proc. Amer. Math. Soc.*, **12**, 1961, p. 657-660).

[14] Lang, S., On quasi-algebraic closure (*Annals of Maths.*, **55**, 1952, p. 373-390).

[15] Lang, S., Algebraic groups over finite fields (*Amer. Journal of Maths.*, **78**, 1956, p. 555-563).

[16] Lang, S., Some theorems and conjectures in diophantine equations (*Bull. Amer. Math. Soc.*, **66**, 1960, p. 240-249).

[17] Lang, S., et Tate, J., Principal homogeneous spaces over abelian varieties (*Amer. Journal of Maths.*, **80**, 1958, p. 659-684).

[18] Ono, T., Arithmetic of algebraic tori (*Annals of Maths.*, **74**, 1961, p. 101-139).

[19] Rosenlicht, M., Some rationality questions on algebraic groups (*Annali di Matematica*, **43**, 1957, p. 25-50).

[20] Serre, J-P., Corps locaux, *Act. Sci. Ind.*, n° 1296, Hermann, 1962.

[21] Springer, T., Sur les formes quadratiques d'indice zéro (*Comptes Rendus*, **234**, 1952, p. 1517-1519).

[22] Springer, T., On the equivalence of quadratic forms (*Proc. Acad. Amsterdam*, **62**, 1959, p. 241-253).

[23] Weil, A., On algebraic groups and homogeneous spaces (*Amer. Journal of Maths.*, **77**, 1955, p. 493-512).

[24] Weil, A., Adeles and algebraic groups (notes by M. Demazure and T. Ono), Inst. Adv. St., Princeton, 1961.

[25] Witt, E., Theorie der quadratischen Formen in beliebigen Körpern (*Journal de Crelle*, **176**, 1936, p. 31-44).